

AMENDMENT TO THE CLAIMS

1. (Currently amended) A method for designing an LSI, comprising the step of encrypting provided circuit design data, the encrypting step includes the steps of:

generating dummy circuit design data;

converting the circuit design data into encrypted circuit design data by combining the circuit design data and the dummy circuit design data; and

generating key data, wherein the encrypted circuit design data does not operate as targeted without inputting the key data into the LSI.

2. (Currently amended) ~~The method according to claim 1,~~ A method for designing an LSI, comprising the step of encrypting provided circuit design data,

wherein the encrypting step includes the step of conducting circuit conversion to produce an encrypted circuit, the circuit conversion being conducted using an entire circuit represented by the circuit design data or a part of the circuit as an original circuit,

the circuit conversion step includes the steps of

providing at least one dummy circuit in parallel with the original circuit, the dummy circuit having a same number of inputs and a same number of outputs as those of the original circuit,

providing a permutation circuit for permutating respective outputs of the original circuit and the dummy circuit, and

providing a selector responsive to a selection signal for selecting a number of signals corresponding to the number of outputs of the original circuit from an output of the permutation circuit so as to produce the encrypted circuit, wherein the selection signal is used as

a key signal, and such a value of the key signal that the output of the original circuit matches an output of the selector is used as a key of the encrypted circuit.

3. (Original) The method according to claim 2, wherein the encrypting step includes the step of producing the dummy circuit to be used in the circuit conversion step, and

the dummy circuit producing step includes

the steps of producing a dummy logic database for the original circuit according to a conversion rule, the dummy logic database including candidate dummy circuits, and

selecting the dummy circuit from the dummy logic database according to an output rule.

4. (Original) The method according to claim 3, wherein the conversion rule includes at least one of inversion of a logic value, conversion of a logic operator, and permutation of logic operators.

5. (Original) The method according to claim 3, wherein the output rule is random selection.

6. (Original) The method according to claim 2, further comprising the step of conducting layout of the encrypted circuit, the layout step including the step of conducting the layout such that an input signal line of the key signal can be connected to either one of a power supply and a ground.

7. (Original) The method according to claim 6, wherein the layout step includes the step of connecting the key signal to one of the power supply and the ground according to the key so as to produce layout of the original circuit.

Application No.: 09/779,440

8-23. (Canceled)